REMARKS

Claims 1-13 and 15-25 are pending in the present application. Claims 1 and 13 are independent.

35 U.S.C. § 103(a) Rejections

Claims 1-13 and 15-25 have been rejected under 35 U.S.C. § 103(a) over Ishiguro (European Patent Application EP 0856821) in view of Barlow (US Patent Publication No 2004/0215964). Applicants respectfully disagree. Claims 1-13 and 15-25 include features that are neither taught nor suggested by the art of record. For example, claim 1 recites:

> A method for checking a digital signature, involving a microcircuit connectable to a data processing system, the microcircuit being designed to receive requests to check digital signatures from the data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key, said method comprising a step of **storing a certificates table containing a digest form of at least one public key in a memory in the microcircuit**, and a phase of checking a digital signature comprising steps of:
>
> receiving by the microcircuit a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked, **calculating a digest form of the received public key, and searching for the calculated digest form of the public key in the certificates table, and decrypting the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.**

Ishiguro teaches an IC card having a memory with a master public key, two secret card keys, a card public key, a card identification number and a first master digital signature (Ishiguro, (57)). Ishiguro further teachers an IC card terminal with memory that stores a master public key, two terminal secret keys, a terminal public key, a terminal identification number, and a second master digital signature (Id.). The terminal is able to authenticate the IC by receiving the cards stored first digital signature, card public key and identification number, and decrypting the digital signature using the public key. If valid, the terminal sends the IC card the second digital signature, the terminal identification number, and the terminal public key, and the IC card similarly validates the terminal. (Id.).

Claim 1 teaches first generating a digest form of the public key (e.g., a hash). This calculated digest is searched for among the digest forms of public keys in the certificates table. If a match is found (e.g., the digest form of the public key is in the certificates table), then the digital signature is decrypted. If the digest form of the public key does not match a digest form of the public key in the certificates table, then no decryption takes place. Thus, the method of claim 1 saves computing resources by only decrypting the digital signature if the digest form of the public key matches a digest form of a public key in the certificates table. These features are not described anywhere in the cited references.

Applicants respectfully submit that Ishiguro fails to teach or suggest "calculating a digest form of the received public key" as taught by claim 1. In the rejection to claim 1, the Examiner states that Ishiguro teaches such a feature at column 2, lines 45-58 (Office action, page 3). Applicants respectfully disagree. The cited portion of Ishiguro merely describes a method for verifying that a digital signature was attached to a document by a party. A digital signature is created from a document using a secret key Q by a first party, and the document and the digital signature are provided to a second party (Ishiguro, column 2, lines 45-49). The second party uses a public key U to verify that the digital signature was created from the document by someone having the secret key Q (Ishiguro, column 2, lines 49-55). There is no mention of calculating a digest form of a received public key anywhere in Ishiguro.

Further, Applicants respectfully submit that Ishiguro fails to teach or suggest "storing a certificates table containing a digest form of at least one public key in a memory in the microcircuit" as taught by claim 1. In the rejection to claim 1, the Examiner implies that "master public key nA" is the same as a digest form of at least one public key. Applicants disagree. As taught in the specification at page 7, for example, a digest is obtained from a public key using a "hashing function, such as MD4 or 5 (Message Digest), SHA (Secure Hash Algorithm) or HMAC (Hashed Message Authentication Code)." Thus, Applicants respectfully submit that a of at least one public key cannot be the same as a public key, and "master public key nA" is not a digest form of at least one public key as suggested by the Examiner.

The Examiner admits that Ishiguro fails to teach or suggest "searching for the calculated digest form of the public key in the certificates table." (Office Action, page 4). However, the Examiner states that Barlow teaches such a feature at paragraphs 56 and 57. Applicants respectfully disagree. The cited portion of Barlow describes a EEPROM for storing two asymmetric pairs of public and private keys (Barlow, paragraph 57). In addition, one or more certificates are stored in the EEPROM, the certificates comprising a card ID, public keys, and a signature of a certifying authority (Id.). Applicants respectfully submit that there is no mention of "searching for the calculated digest form of the public key in the certificates table" or a "digest form of a public key" anywhere in the cited portion of Barlow. Applicants respectfully submit that the stored certificate of Barlow is not a digest of a public key, nor is there any mention in Barlow of the certificate including a digest of a public key.

Because Ishiguro and Barlow, alone or in combination, fail to teach or suggest each and every feature of claim 1, they cannot possibly render claim 1 obvious. Applicants therefore respectfully request that the Examiner withdraw the rejection and allow claim 1.

Claim 13 contains features that are similar, but not identical to the features described above for claim 1, and is therefore allowable for at least the reasons given for claim 1. Applicants therefore respectfully request that the Examiner withdraw the rejections and allow claim 13.

Claim 3 is dependent on claim 1, and is therefore allowable for at least the reason given above for claim 1. Moreover, claim 3 contains additional features that are neither taught nor suggested by the art of record. Claim 3 recites "the phase of inserting a public key in the certificates table comprises a step of inserting in the certificates table of a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key." In the rejection of that claim, the Examiner states that such a feature is taught by Barlow at paragraph 45 (Office Action, page 5). Applicants respectfully disagree. The cited portion of

Barlow merely describes the process of adding or deleting a public key and possibly its certificate from the EEPROM, but makes no mention of "inserting in the certificates table of a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted" nor inserting a pointer of any kind. Moreover, the cited portion of Barlow does not teach anything similar to "defin[ing] a certification tree." Applicants therefore respectfully request that the Examiner withdraw the rejection and allow claim 3.

Claims 2, 4-12, and 15-25 are variously dependent on claims 1, 3 and 13, and are therefore allowable for at least the reasons given for claims 1, 3 and 13. Applicants therefore respectfully request that the Examiner withdraw the rejection and allow claims 2, 4-12, and 15-25.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants submit that all claims are in condition for allowance.

Please apply any required charges or any credits to deposit account 06-1050 referencing the above Attorney Docket No.

Respectfully submitted,

Date: 9/18/2008

Michael W. Tieff
Reg. No. 57,845

Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 66550-1022
Telephone: (302) 652-5070
Facsimile: (877) 769-7945

80066288.doc